UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/836,214	04/18/2001	Peter T. Dinsmore	NAI1P089/00.175.01	6427

28875 7590 05/29/2007

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
05/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/836,214	DINSMORE ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-15,17-21,28-30 and 38-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-15,17-21,28-30 and 38-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 22 January 2007, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

2. To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

3. A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Gilberto Barron, Jr.
Supervisory Patent Examiner
Art Unit 2132

4. Claims 1-9, 11-15, 17-21, 28-30, and 38-41 have been presented for examination.

5. Claims 10, 16, 22-27, and 31-37 have been cancelled as per Applicant's request.

Response to Arguments

6. Applicant's arguments with respect to claims 1-9, 11-15, 17-21, 28-30, and 38-41 have been considered but are moot in view of the new ground(s) of rejection.

Specification

7. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter of claim 39, specifically a computer-usable medium. Since the Applicant failed to define the computer usable medium in the specification, it is impossible to ascertain the intended scope of the claim. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction is required.

8. The amendment filed 10 May 2006 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: "wherein said updating does not use new secret information."

9. Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

11. Claims 1-9, 11, 12, 28-30, and 38-41are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. The Applicant has provided no discussion of excluding the generation of new secret information as Applicant alleges on page 7 of Applicant's Appeal Brief of 22 January

2007. Since the Applicant fails to provide any discussion stating that the updating occurs without generating new secret information, it constitutes new matter and fails to comply with the written description requirement.

Claim Rejections - 35 USC § 101

12. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

13. Claim 39 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 39 requires a computer-usable medium, which, as noted above, the Applicant has failed to define in the specification. One of ordinary skill could reasonably conclude that the usable medium includes transmission media and carrier waves since the invention is implemented in a distributed, networking environment. The Office's current position is that claims involving signals encoded with functional descriptive material do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. *See* 1300 OG 142 (November 22, 2005) (in particular, see Annex IV(c)).

Claim Rejections - 35 USC § 102

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

15. Claims 1-8, 11-15, 17-21, 28-30, and 38-41 are rejected under 35 U.S.C. 102(b) as being anticipated by **Dynamic Cryptographic Context Management (DCCM): Report #1 Architecture and System Design**, by David M. Balenson et al., hereinafter Balenson.

16. As per claim 1, Balenson discloses an environment that includes a plurality of users, wherein each user possess secrets that are shared by respective sets of said plurality of users, a secret updating method, comprising:

(a) updating at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by said at least one evicted user (pages 40, 52, 61, 113, 114, i.e. updating group key in response to an eviction), wherein said updating does not use new secret information (p. 99, i.e. pre-distributed secret information is used to compute a key without any new key being transmitted).

17. Regarding claim 2, Balenson teaches wherein said updating comprises updating a plurality of compromised secrets (pages 9-11, 18-22, 51-63 [i.e. **Group Key Management**], 115, i.e. multiple evictions require multiple key updates).

18. Regarding claim 3, Balenson discloses wherein said updating comprises updating all compromised secrets (pages 9-11, 18-22, 51-63 [i.e. **Group Key Management**], 115, i.e. multiple evictions require multiple key updates).

19. Regarding claim 4, Balenson discloses wherein said updating comprises updating at least one compromised secret known by one evicted user (pages 9-11, 18-22, 51-63 [i.e. **Group Key Management**], 115, i.e. multiple evictions require multiple key updates).

20. With regards to claims 5, 14, and 15, Balenson teaches wherein said updating occurs upon an eviction event, wherein only said second user or the second user and one or more other users are evicted (page 115, Figure 29).

21. Regarding claim 6, Balenson teaches wherein said updating comprises updating at least one compromised secret known by a plurality of evicted users (pages 40, 52, 61, 113, 114, i.e. updating group key in response to an eviction).

22. With regards to claim 7, Balenson teaches wherein said updating occurs on a periodic basis (page 13).

23. Regarding claim 8, Balenson teaches wherein said updating comprises updating a compromised secret using one non-compromised secret (pages 40, 52, 61, 113, 114).

24. Regarding claim 9, Balenson teaches wherein said updating comprises updating a compromised secret known by a set of users using a non-compromised secret of a subgroup of said set of users (Figure 4, pages 18, 20).

25. Regarding claim 11, Balenson teaches wherein said compromised secret is shared by said plurality of users (pages 40, 52, 61, 113, 114).

26. Regarding claim 12, Balenson teaches wherein said secrets enables secure communication (page 1).

27. As per claim 13, Balenson teaches an environment that includes a plurality of users, wherein a first user possesses a set of keys, said set of keys including a first key that enables secure communication among a set of sets, said set of users including at least said first user and a second user, a keying method, comprising:

(a) upon eviction of at least said second user (pages 49, 115, 117), determining an updated first key using information that includes said first key and a second key (page 10, i.e. one-way function tree the keys are computed up, so in Figure 2 the keys for 1 and 2 are used to compute the key for D), wherein said second key enables secure communication among a subgroup of said set of users (page 1), wherein said subgroup does not include users subject to said eviction (Figure 4, pages 18, 20)

(1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key (page 99, i.e. prevent collusion).

28. With regards to claims 17 and 41, Balenson teaches wherein said determining uses a one-way function (page 10, Figure 2, i.e. one-way function tree).

29. Concerning claim 18, Balenson teaches wherein F() is a one-way function (page 10, Figure 2, i.e. one-way function tree).

30. Regarding claim 19, Balenson teaches wherein said determining uses only said first key and said second key (page 10, Figure 2, i.e. binary trees only account for two child nodes).

31. Regarding claims 20 and 21, Balenson teaches wherein said subgroup includes only said first user or a plurality of users (Figure 4, pages 18, 20).

32. As per claim 28, Balenson teaches a keying method in an environment having a plurality of users, each user being capable of storing a set of keys that enable secure communication among sets of said plurality of users, comprising:

(a) distributing first information that enables users to update, after eviction of one or more users, a set of compromised keys that are known to said one or more users without receiving new key information (pages 40, 52, 61, 113, 114, i.e. updating group key in response to an eviction), wherein said update does not include new secret information (p. 99, i.e. pre-distributed secret information is used to compute a key without any new key being transmitted).

33. Regarding claim 29, Balenson discloses wherein said first information includes information that enables identification of a one-way function (page 10, Figure 2, i.e. one-way function tree).

34. Regarding claim 30, Balenson teaches wherein said first information includes information that enables identification of said evicted one (pages 112, 113) or more users (page 114).

35. As per claims 38 and 39, Balenson discloses a secret sharing system, comprising:

a key server that distributes secret information to a plurality of users (page 40, Figure 5), wherein each user is sent secrets that are shared by respective sets of said plurality of users (page 99, i.e. pre-distributed secret information is used to compute a key without any new key being transmitted), said key server being operative to update at least one compromised secret known by at least one evicted user (pages 40, 52, 61, 113, 114, i.e. updating group key in response to an eviction) at least one non-compromised secret that is not known by said at least one evicted user (page 99, i.e. pre-distributed secret information is used to compute a key without any new key being transmitted).

36. Regarding claim 40, Balenson discloses wherein said non-compromised secret utilized for said updating is known by all users in said plurality of users and is not known by said at least one evicted user (page 99, i.e. prevent collusion).

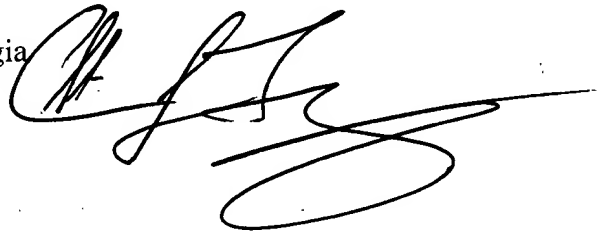
Conclusion

37. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

38. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

39. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131



clf